Tech Data
Advanced Solutions

# SECURITY SALES GUIDE

## So positionieren Sie Endpoint Management erfolgreich bei Ihren Kunden – als Lösung oder Service.

# Endpoint Management – die Basis der IT-Security

Rechner und Server im Unternehmen sind wie ein Zuhause für digitale Daten. Jede Anwendung, die Sie auf Ihrem Computer installieren, ist ein Erweiterungsbau. Dumm nur, dass die Bauunternehmen jeden Anbau in unterschiedlicher Qualität und Technik bauen.

Wenn Ihnen eines Tages ein Bauunternehmer eines Anbaus mitteilt, dass er ein unentdecktes Sicherheitsrisiko in einem seiner Gebäudezugänge hinterlassen hat, ist Ihr schönes Zuhause plötzlich nicht mehr sicher.

Fehler im Programm oder nicht installierte Software-Aktualisierungen sind im übertragenen Sinne die offene Tür Ihres Hauses und stellen für Unternehmen ein großes Risiko dar. Sie sind das Einfallstor für Hacker und Malware in Unternehmen und daher ist Endpoint-Patch-Management die Grundlage für alle IT-Security Konzepte.

# Erste Hilfe für Ihren Kundentermin

## Elevator Pitch

„Für ein gutes Sicherheitskonzept müssen Sie in der Lage sein, die Schwachstellen Ihrer Systeme in Sekundenschnelle zu erkennen und zu beheben. Mangelnde Transparenz und Kontrolle macht Ihr Unternehmen anfällig für Angriffe. Die Frage ist nicht, ob Sie Opfer einer Sicherheitsverletzung werden, sondern wann und wann Sie es merken. Denn in der Regel bleibt kein aufgebrochenes Schloss oder ein zertrümmertes Fenster zurück.“

## Mit diesen Fragen können Sie das Gespräch eröffnen:

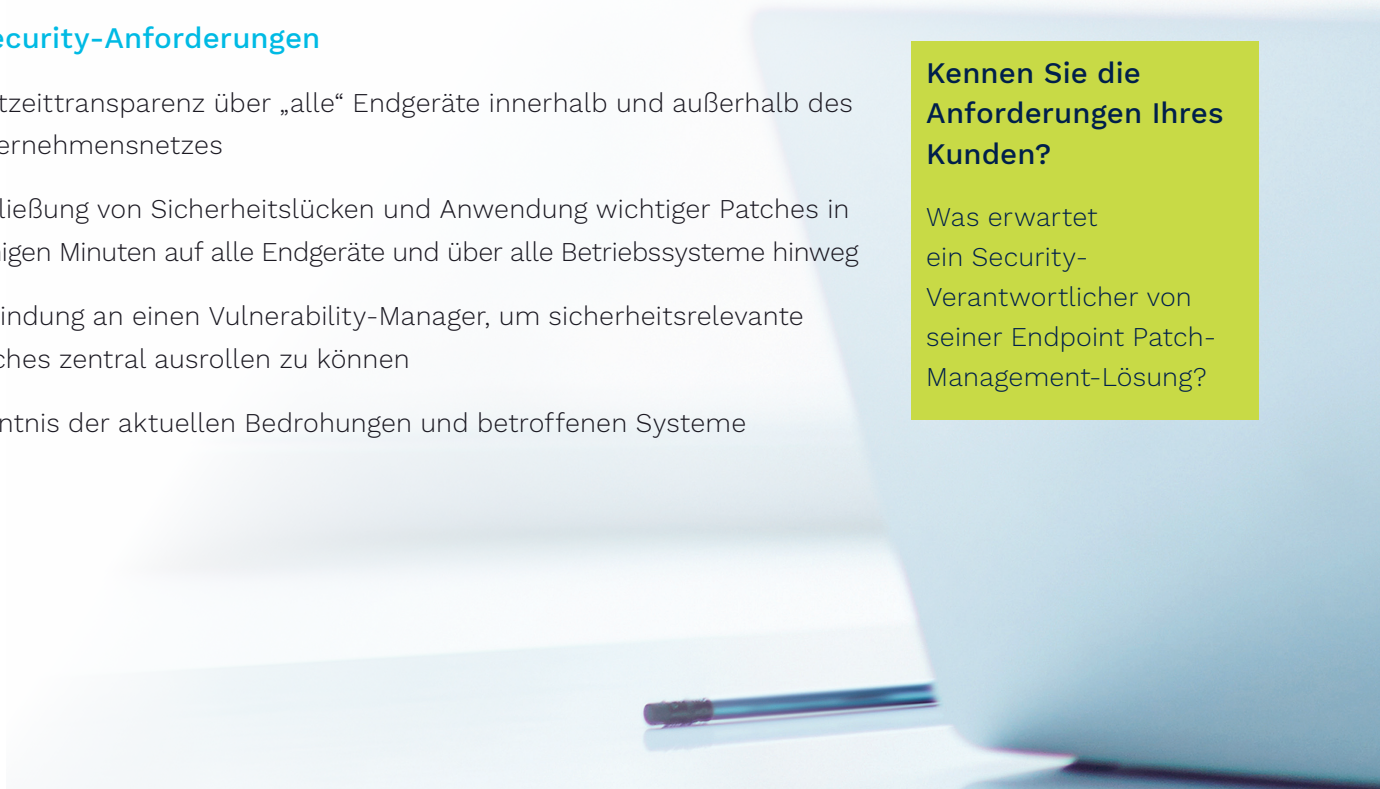
- Setzen Sie aktuell Patch-Management in Ihrem Unternehmen ein?
- Sind Ihre Unternehmens-Audits aufwendig und anstrengend?
- Haben Sie Auflagen (BaFin, Datenschutz, IT-Sicherheitsgesetz, GDPR, etc.)?
- Welcher Schaden entsteht, wenn Ihre wichtigsten Daten manipuliert / gestohlen werden?

## Die Security-Anforderungen

1. Echtzeittransparenz über „alle“ Endgeräte innerhalb und außerhalb des Unternehmensnetzes
2. Schließung von Sicherheitslücken und Anwendung wichtiger Patches in wenigen Minuten auf alle Endgeräte und über alle Betriebssysteme hinweg
3. Anbindung an einen Vulnerability-Manager, um sicherheitsrelevante Patches zentral ausrollen zu können
4. Kenntnis der aktuellen Bedrohungen und betroffenen Systeme

**Kennen Sie die Anforderungen Ihres Kunden?**

Was erwartet ein Security-Verantwortlicher von seiner Endpoint Patch-Management-Lösung?



## Die Operations-Anforderungen

1. Schnelles Ausrollen von Software-Installationen im gesamten Unternehmen: in wenigen Stunden statt Wochen oder Monaten auf hunderttausenden Microsoft Windows-, Mac OS-, UNIX- sowie Linux Geräten
2. Automatisches Aufspüren von Rechnersystemen im kompletten Unternehmen sowie automatische Dokumentation der Systeme inklusive der installierten Software
3. Management über den kompletten Software Lifecycle – vom Kauf bis zur Stilllegung – einschließlich Sicherheitskonformität und Patch-Management
4. „User“-rollenbasiertes Management, welches das Lizenzmanagement deutlich erleichtert
5. Überwachung von Software, Prozessen und Dateisystemen sowie der Hardwarenutzung zur Sicherstellung der Prüfbarkeit bei Audits. Diese Funktionalität sorgt zudem für geringere Lizensierungskosten durch die Ermittlung ungenutzter Software.

# So positionieren Sie IBM BigFix

IBM BigFix ist eine marktführende Endpoint-Management- und Sicherheitsplattform, mit der IT-Abteilungen Betriebskosten senken, Endpoint-Management-Zyklen verkürzen und Compliance in Echtzeit durchsetzen können.

Welches Betriebskonzept Sie Ihrem Kunden anbieten möchten, bleibt bei BigFix Ihnen überlassen: ob als eine von Ihnen gemanagte Lösung oder lediglich als Service. Durch seine Mandantenfähigkeit und die Integration in das IBM Immunsystem - ein ganzheitliches Sicherheitskonzept - ist IBM BigFix für Managed Service Provider eine Bereicherung.

## Für welche Kunden ist IBM BigFix geeignet?

**Unternehmensgröße**: ab 30 Mio. Euro Umsatz; ab 150 Mitarbeiter

**Branchen**: Banken, Chemie und Erdöl, Bildung, Energie und Versorgung, Finanzmärkte, Regierung, Gesundheitswesen und Biowissenschaften, Versicherungen, Einzelhandel, Reise und Transportwesen

**Funktion**: CIO, CISO, VP/Director - FP&A, Director of IT-Security, VP of IT, Security and Risk

**Kundenbedürfnis**: Das Unternehmen benötigt eine Reaktion in Echtzeit auf Vorfälle über alle Endpunkte hinweg.

## Die wichtigsten Argumente für den Gesprächseinstieg:

CISOs und/oder Senior Executives sind verantwortlich für die Sicherheit: Sie müssen in der Lage sein, Schwachstellen innerhalb von Minuten über alle Endpunkte hinweg zu finden und zu beheben - innerhalb und außerhalb des Unternehmensnetzwerks.

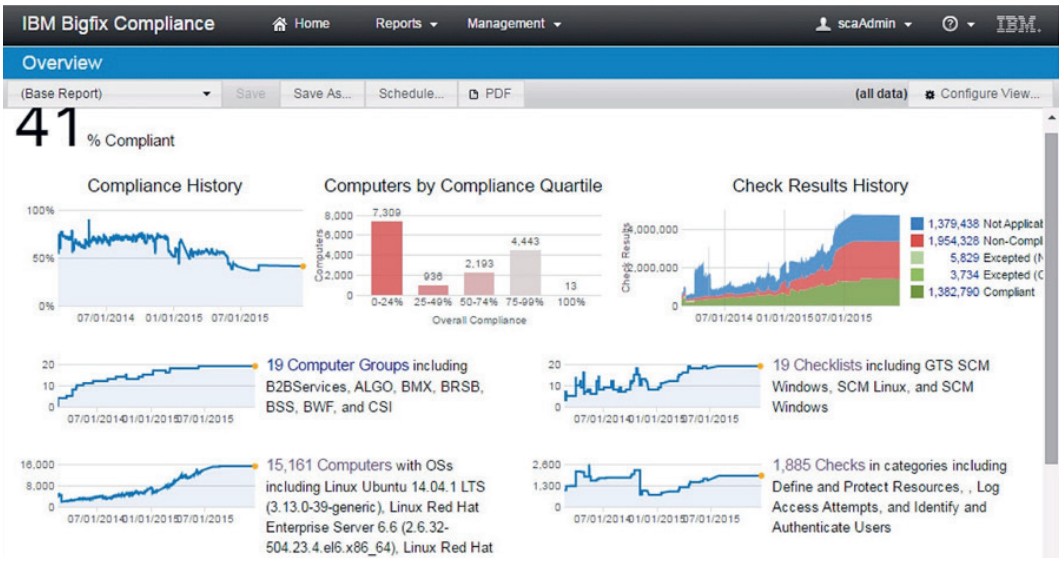
Im Hinblick auf Sicherheit, Compliance & Risiko müssen sie die “Time to Compliance” beschleunigen. Mit einem gemeinsamen Tool/Reporting zur Behebung von Risiken können sie Audits erfolgreich bestehen.

# Welche Module bietet IBM BigFix?

| COMPLIANCE | LIFECYCLE | INVENTORY | PATCHING |
|---|---|---|---|

## COMPLIANCE

**BigFix Compliance** stellt unternehmensweit die kontinuierliche Einhaltung von Sicherheitsrichtlinien für jeden Endpunkt innerhalb und außerhalb des Unternehmensnetzes sicher. Der sofortige Support für die gängigsten Sicherheitsbenchmarks (CIS, DISA STIG, USGCB und PCI-DSS) ist eingeschlossen. Ein intelligenter Agent überwacht, erzwingt und dokumentiert den Status der Sicherheitskonfiguration der Endpunkte in Echtzeit. Und das unabhängig von Betriebssystem und Ort.




Quelle: https://www.ibm.com/de-de/marketplace/bigfix-compliance

Compliance-Abweichungen werden sofort gemeldet und können in kürzester Zeit behoben werden, um die Sicherheitsrisiken insgesamt zu reduzieren. Dabei werden nur die richtigen Patches angewandt.

### FRAGEN AN DEN KUNDEN

- Sind Ihre Unternehmensaudits aufwendig und anstrengend?
- Welche Konsequenzen haben Auditverstöße für Sie und Ihr Unternehmen?

## LIFECYCLE

**BigFix Lifecycle** hilft, Probleme innerhalb von Minuten zu finden und zu beheben – auf allen Endgeräten: ob fest verkabelt, mobil, physisch oder virtuell. Damit können Hunderttausende von Endgeräten mit mehr als 90 verschiedenen Betriebssystem-Versionen innerhalb von Stunden oder sogar Minuten ermittelt, geschützt und gemanged werden. Die Lösung stellt sicher, dass alle Systeme über die neuesten Patches verfügen und sicher sind. Außerdem können Betriebssystem-Migrationen automatisiert und Endgeräte in Echtzeit abfragt werden.

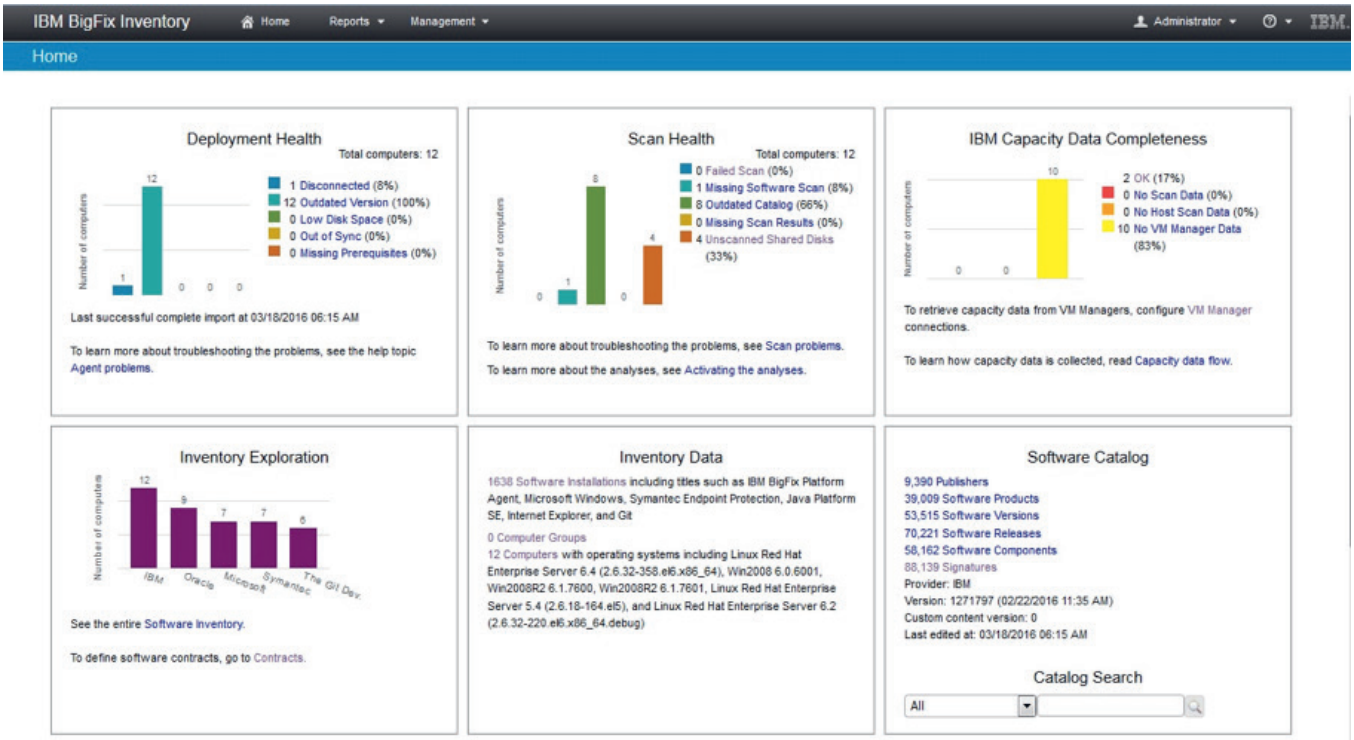
So können bösartige Dateien ermittelt, Software schnell installiert, komplexe Aufgaben automatisiert oder eine einfache Remote-Steuerung mit nur wenigen Klicks durchgeführt werden. Über eine benutzerfreundliche Webschnittstelle mit einfachen intuitiven Fragen kann BigFix Query Endgeräte präzise erkennen und prüfen.

### FRAGEN AN DEN KUNDEN

- Wissen Sie, zu welchen aktuellen Bedrohungen es einen Patch gibt?
- Sind Sie in der Lage, die Systeme, die in Ihrer Verantwortung liegen, zeitnah zu patchen?

## INVENTORY

**BigFix Inventory** kann den Zeitaufwand für eine umfassende Inventarisierung von Software-Assets zu Lizenzabgleichs- oder Compliance-Zwecken erheblich verkürzen. Die Lösung zeigt, welche Assets Eigentum des Unternehmens sind, welche installiert, aber nicht Eigentum des Unternehmens sind und wie häufig die Software genutzt wird. BigFix Inventory unterstützt eine bessere Planung, Budgetierung und Lizenzeinhaltung und mindert gleichzeitig das Sicherheitsrisiko.




Quelle: https://www.ibm.com/de-de/marketplace/bigfix-inventory

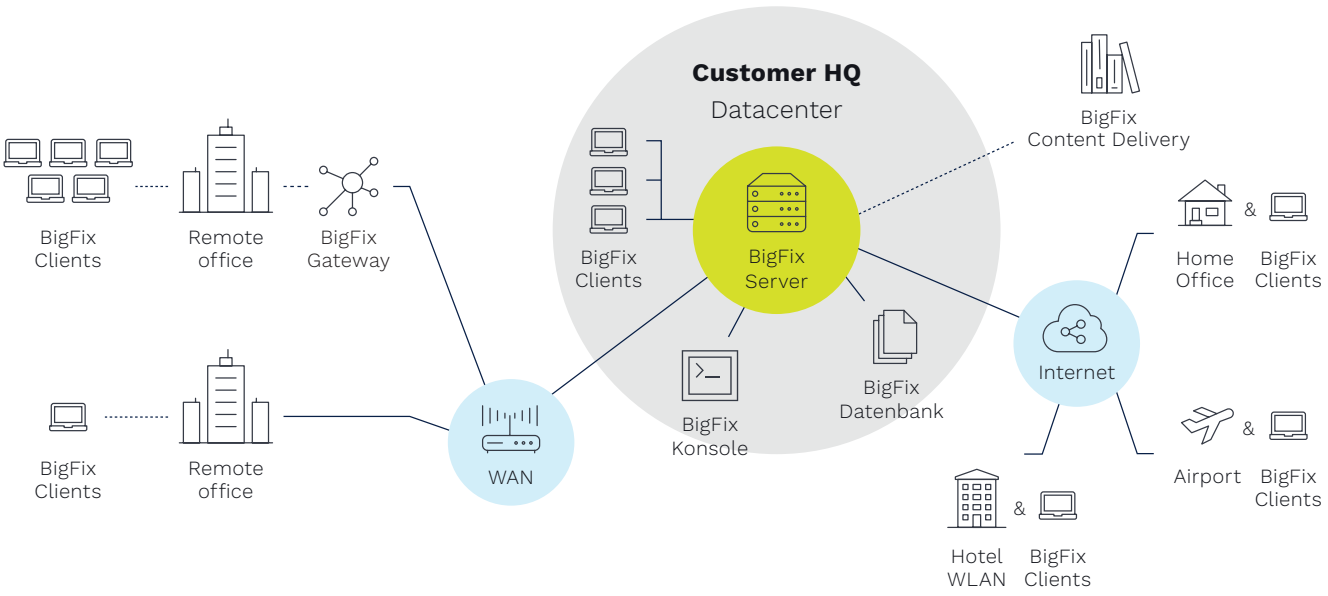
### FRAGEN AN DEN KUNDEN

- Haben Sie die Kontrolle über Ihre Lizenzen und den echten Bedarf Ihrer Mitarbeiter?
- Wie viele Lizenzen in Ihrem Unternehmen werden nicht aktiv genutzt und was können Sie sparen?
- Welche Software läuft auf Ihren Systemen und haben Sie die Lizenz erworben?

## PATCHING

**BigFix Patch** stellt einen automatisierten, vereinfachten Patching-Prozess bereit, der von einer einzigen Konsole aus gesteuert wird. Die Lösung bietet Transparenz in Echtzeit und erlaubt die Durchsetzung von Richtlinien. Sie hilft, Patches auf Endgeräten – innerhalb und außerhalb des Unternehmensnetzes – einzuspielen und zu verwalten. Bereits beim ersten Patch-Durchlauf konnten Kunden Erfolgsquoten von 98 Prozent verzeichnen. Die Lösung steigert nicht nur die Effektivität des Patch-Prozesses, sondern senkt zudem die Betriebskosten und verringert die Patch-Zykluszeiten für den Schutz der Endgeräte.

# Wie sieht die Infrastruktur von BigFix aus?




## BigFix-Server

Der BigFix-Server bildet das Herzstück der BigFix-Infrastruktur. Er koordiniert den Datenfluss von und zu den einzelnen Rechnern.

## BigFix-Konsole

Die BigFix-Konsole bietet eine systemweite Sicht auf alle Rechner in der Infrastruktur und deren Konfiguration. Sie wird verwendet, um Computer mit bestimmten Aktionen wie der Installation des Scanners oder der Planung von Software- und Kapazitäts-Scans anzusprechen.

## BigFix-Client

Der BigFix-Client ist für alle Produkte, die auf der BigFix-Plattform basieren, vorgesehen und sollte auf jedem Computer - einschließlich Backup- und Recovery-Maschinen - installiert werden, um die Revisionssicherheit zu gewährleisten. Der BigFix-Client läuft auf allen von BigFix-Inventory unterstützten Betriebssystemen.

## Webberichte

Web Reports sind eine High-Level-Webanwendung, die die Visualisierung von Daten aus der BigFix-Infrastruktur ermöglicht.

## Datenbanken

BigFix-Server und BigFix Inventory Server benötigen ihre eigenen Datenbank-Instanzen.

# Was ist der USP der Lösung?

## IBM BigFix ist Leader im Gartner Magic Quadrant

Enterprise Mobility Management (EMM) ist der “Klebstoff”, der mobile Geräte mit der Unternehmensinfrastruktur verbindet. Der Gartner Magic Quadrant für EMM 2017 positioniert IBM im Leaders-Quadranten.


Quelle:
https://techorchard.com/wp-content/uploads/2017/07/Gartner_MagicQuadrant_EMM_2017.pdf

## IBM BigFix ist eine integrierte Lösung

IBM BigFix kann zusammen mit IBM QRadar und IBM MaaS360 zu einem schlagkräftigen IT-Security Konzept ausgebaut werden. Denn moderne Angriffe werden heute nicht mehr von einer einzigen Firewall abgewehrt. Es braucht ein fein abgestimmtes Orchester an Lösungen, die miteinander integriert sind. Nur die schnelle Weitergabe von Informationen zu Status und Bedrohung schafft heutzutage die nötige IT-Sicherheit.

Das IBM SIEM System QRadar bildet das Kernstück dieses Konzepts und beinhaltet ein Dashboard „Manage Vulnerable Computers“. Dieses führt eine Risikobewertung für jedes System im Unternehmen durch, das durch IBM BigFix verwaltet wird.

Anhand der aufbereiteten Daten zur Risikobeurteilung von QRadar erkennt man sofort, welche Computer am gefährdetsten sind. Im Dashboard gibt es eine Liste der für CVEs (Common Vulnerabilities and Exposures) verfügbaren Patches. Die Patches können vom Dashboard ausgeführt werden, um die gefährdeten Computer zu schützen. Mit IBM Maas360 werden diese Fähigkeiten auch in die mobile Welt übertragen, damit volle Kontrolle über Patches und Applikationen auch auf den mobilen Endgeräten besteht.

# Zusammengenfasst

Durch die Kombination von QRadar und BigFix können Kunden:

- ihre Sicherheitsrichtlinien auf Endgeräte unabhängig von deren Ort erweitern
- Richtlinien bei Sicherheits-, Regulierungs- und Betriebsvorschriften kontinuierlich durchsetzen
- Schwachstellen-Patching auf der Grundlage von Risiken priorisieren

## Details für den Abschluss des Projekts

**Die wichtigsten Kennzahlen:**

| **Kundengröße:** | **Typische Projektgröße:** | **Typisches Partner Incentive:** | **Typische Projektlaufzeit:** |
|---|---|---|---|
| Ab 150 Geräten -> kein Limit nach oben | 15.000 € - 2.000.000 € | 20% | 3-9 Monate |

## IBM BigFix –
## perfekt für die Bereitstellung eines Managed Services

Die Lösung kann von Ihnen auch als Managed Service betrieben werden. Jedes Unternehmen muss sich ernsthaft mit IT-Security auseinandersetzen und kann die Frage nach Sicherheit nicht mehr nur oberflächlich beleuchten. Bei der genaueren Betrachtung ihrer IT-Security-Anforderungen stoßen viele Unternehmen an Grenzen. Gutes Personal zu finden, das die Lücken schließen könnte, ist zeitaufwendig und sehr teuer. Was ihnen bleibt, ist die Expertise extern zu suchen und IT-Dienstleister zu beauftragen. Mit IBM BigFix haben Sie hervorragende Möglichkeiten, sich als Managed Service Provider bei Ihren Kunden zu positionieren.

## So unterstützt Sie Tech Data im kompletten Vertriebsprozess

Unsere Experten widmen sich mit ihrer langjährigen Erfahrung und einem ausgereiften Portfolio aus branchenführenden und innovativen Lösungen der IT-Security in Ihrem Unternehmen. So können wir Sie im gesamten Vertriebsprozess unterstützen. Unsere technischen Teams erklären hierbei stets verständlich und bedarfsorientiert die Vorzüge der einzelnen Produkte und erarbeiten gemeinsam mit unseren Sales Mitarbeitern ein individuelles auf Sie abgestimmtes Konzept zur nachhaltigen Sicherung der Unternehmensdaten Ihrer Kunden.

Wir begleiten Sie von Ihrer Ausbildung, über die Lead-Generierung bis hin zum Proof-of-Concept. So können Sie sich voll und ganz auf die Anforderungen Ihrer Kunden konzentrieren.

## Platz für Ihre Notizen

Tech Data
Advanced Solutions

## Ihre Ansprechpartner

**Patrick Olschewski**
Business Development Manager
patrick.olschewski@techdata.com

**Siegfried Markiefka**
Business Development Manager
smarkiefka@techdata.de